Отчёт по лабораторной работе №3

дисциплина: Информационная безопасность

Быстров Глеб Андреевич

Содержание

# 1 Цель работы

В данной лабораторной работе мне будет необходимо получить практические навыки работы в консоли с атрибутами файлов для групп пользователей.

# 2 Задание

Последовательно выполнить пункты по настройке доступа через команды в терминале для двух пользователей.

# 3 Теоретическое введение

В Linux у каждого файла и каждого каталога есть два владельца: пользователь и группа.

Эти владельцы устанавливаются при создании файла или каталога. Пользователь, который создаёт файл становится владельцем этого файла, а первичная группа, в которую входит этот же пользователь, так же становится владельцем этого файла. Чтобы определить, есть ли у вас как у пользователя права доступа к файлу или каталогу, оболочка проверяет владение ими. [1].

Выделяют три категории пользователей, которым могут предоставляться права на файл:

* Сам владелец (u – user) объекта – конкретный пользователь, чье имя числится в атрибутах файла как имя владельца этого файла. Обычно если пользователь создает файл, то он автоматически записывается как его владелец.
* Группа (g – group), к которой принадлежит владелец файла. Когда в Linux создается пользователь, то для него создается одноименная группа. Однако средствами администрирования системы можно объединять пользователей в различные группы. При этом конкретный пользователь может входить в состав нескольких групп. Группы позволяют предоставлять права доступа к ресурсам сразу нескольким людям, но при этом ограниченному кругу лиц.
* Все остальные (o – other) – это все те, кто не является владельцем файла и не принадлежит к группе владельца файла. То есть любой посторонний пользователь.

Чтение, запись, выполнение – это то, что можно делать с существующим файлом, возможные действия над ним. У каждой категории пользователей (владельца, группы, остальных) должны быть свои права на каждое вышеупомянутое действие.

* Право на чтение (r – read) означает, что файл можно просматривать. Например, открыть файл и, если он текстовый, прочитать содержащийся в нем текст. Если это файл изображения, то можно посмотреть изображение. Наличие права только на чтение не позволяет изменять файл. То есть нельзя будет исправить текст или подрисовать что-то к картинке.
* Право на запись (w – write) позволяет изменять файл, то есть дописывать в него информацию или заменять ее другой.
* Право на исполнение (x – execution) имеет смысл не для всех файлов, хотя может быть установлено для любого. Это право позволяет исполнять файл как программу, при этом в файле должны быть записаны инструкции для процессора, то есть файл должен быть исполняемой программой.

Первые три записи – это права владельца, вторые три записи – права группы, последняя тройка – права на файл для всех остальных. Если обозначить каждое право соответствующей буквой, и все права всем предоставляются, то получится такая запись: rwxrwxrwx [2].

Рассмотрим подробнее, что значат условные значения флагов прав:

— - нет прав, совсем;

–x - разрешено только выполнение файла, как программы но не изменение и не чтение;

-w- - разрешена только запись и изменение файла;

-wx - разрешено изменение и выполнение, но в случае с каталогом, вы не можете посмотреть его содержимое;

r– - права только на чтение;

r-x - только чтение и выполнение, без права на запись;

rw- - права на чтение и запись, но без выполнения;

rwx - все права;

–s - установлен SUID или SGID бит, первый отображается в поле для владельца, второй для группы;

–t - установлен sticky-bit, а значит пользователи не могут удалить этот файл [3].

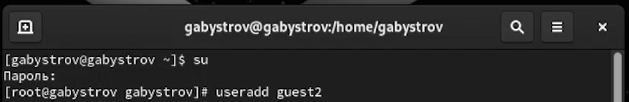
Использование команды ls с опцией -l выведет на экран «длинную» распечатку, в которой будут, среди прочего, отражены права доступа к файлу [4].

Все группы, созданные в системе, находятся в файле /etc/group. Посмотрев содержимое этого файла, вы можете узнать список групп linux, которые уже есть в вашей системе.

Кроме стандартных root и users, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия пользователя, а следовательно, и процесса, запущенного от этого пользователя. Здесь можно считать, что пользователь - это одно и то же что процесс, потому что у процесса все полномочия пользователя, от которого он запущен [5].

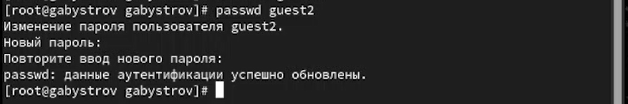
# 4 Выполнение лабораторной работы

1. В установленной операционной системе создал учётную запись пользователя guest2 (использовал учётную запись администратора): useradd guest2 (рис. ??).



Создание новой учетной записи

1. Задал пароль для пользователя guest2 (использовал учётную запись администратора): passwd guest2 (рис. ??).



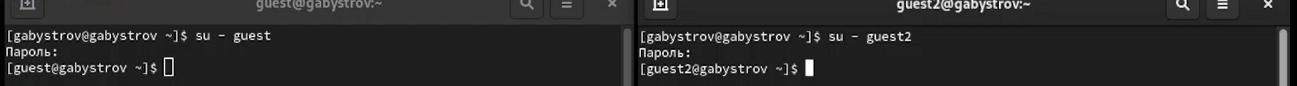
Создание пароля

1. Добавил пользователя guest2 в группу guest: gpasswd -a guest2 guest (рис. ??).

Добавление в группу

Добавление в группу

1. Осуществил вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли (рис. ??).



Вход в систему на разных консолях

1. Для обоих пользователей командой pwd определил директорию, в которой нахожусь. Сравнил её с приглашениями командной строки (рис. ??).

Определение директорий

Определение директорий

1. Уточнил имя моего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определил командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравнил вывод команды groups с выводом команд id -Gn и id -G. (рис. ??).



Информация о пользователях

1. Сравнил полученную информацию с содержимым файла /etc/group. Просмотрел файл командой cat /etc/group (рис. ??).



Просмотр файла

1. От имени пользователя guest2 выполнил регистрацию пользователя guest2 в группе guest командой newgrp guest (рис. ??).

Выполнение регистрации пользователя guest2

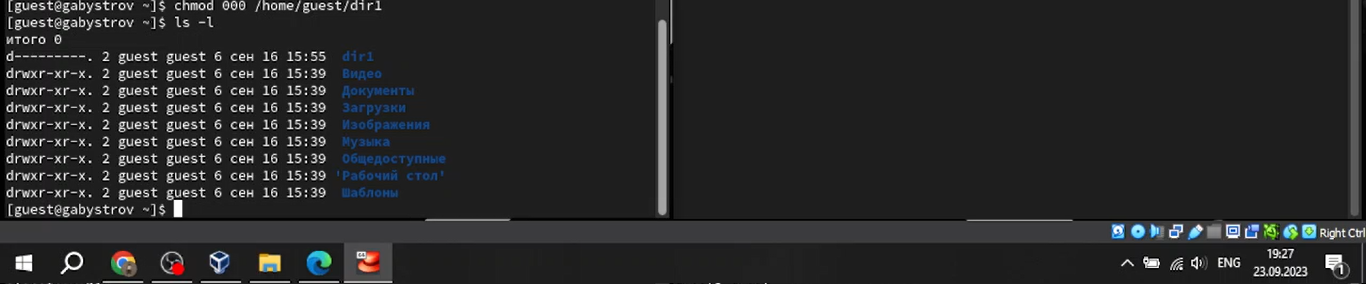
Выполнение регистрации пользователя guest2

1. От имени пользователя guest изменил права директории /home/guest, разрешив все действия для пользователей группы: chmod g+rwx /home/guest (рис. ??).

Изменение прав директории /home/guest

Изменение прав директории /home/guest

1. От имени пользователя guest снял с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl и проверил правильность снятия атрибутов (рис. ??).



Снятие с дирректории всех атрибутов

1. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнил табл. 3.1, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занес в таблицу знак «+», если не разрешена, знак «-». Сравнил табл. 2.1 (из лабораторной работы № 2) и табл. 3.1.

Table 1: Установленные права и разрешенные действия для групп

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| --------- (000) | --------- (000) | - | - | - | - | - | - | - | - |
| --------- (000) | --x------ (010) | - | - | - | - | + | - | - | - |
| --------- (000) | -w------- (020) | - | - | - | - | - | - | - | - |
| --------- (000) | -wx------ (030) | - | - | - | - | - | - | - | - |
| --------- (000) | r-------- (040) | - | - | - | - | - | - | - | - |
| --------- (000) | r-x------ (050) | - | - | - | - | - | - | - | - |
| --------- (000) | rw------- (060) | - | - | - | - | - | - | - | - |
| --------- (000) | rwx------ (070) | - | - | - | - | - | - | - | - |
| --x------ (010) | --x------ (010) | - | - | - | - | + | - | - | - |
| --x------ (010) | -w------- (020) | - | - | + | - | + | - | - | - |
| --x------ (010) | -wx------ (030) | - | - | + | - | + | - | - | - |
| --x------ (010) | r-------- (040) | - | - | - | + | + | - | - | - |
| --x------ (010) | r-x------ (050) | - | - | - | + | + | - | - | - |
| --x------ (010) | rw------- (060) | - | - | + | + | + | - | - | - |
| --x------ (010) | rwx------ (070) | - | - | + | + | + | - | - | - |
| --x------ (010) | --------- (000) | - | - | - | - | + | - | - | - |
| -w------- (020) | --------- (000) | - | - | - | - | - | - | - | - |
| -w------- (020) | --x------ (010) | - | - | - | - | - | - | - | - |
| -w------- (020) | -w------- (020) | - | - | - | - | - | - | - | - |
| -w------- (020) | -wx------ (030) | - | - | - | - | - | - | - | - |
| -w------- (020) | r-------- (040) | - | - | - | - | - | - | - | - |
| -w------- (020) | r-x------ (050) | - | - | - | - | - | - | - | - |
| -w------- (020) | rw------- (060) | - | - | - | - | - | - | - | - |
| -w------- (020) | rwx------ (070) | - | - | - | - | - | - | - | - |
| -wx------ (030) | --------- (000) | + | + | - | - | + | - | + | - |
| -wx------ (030) | --x------ (010) | + | + | - | - | + | - | + | - |
| -wx------ (030) | -w------- (020) | + | + | + | - | + | - | + | - |
| -wx------ (030) | -wx------ (030) | + | + | - | + | + | - | + | - |
| -wx------ (030) | r-------- (040) | + | + | - | + | + | - | + | - |
| -wx------ (030) | r-x------ (050) | + | + | - | + | + | - | + | - |
| -wx------ (030) | rw------- (060) | + | + | + | + | + | - | + | - |
| -wx------ (030) | rwx------ (070) | + | + | + | + | + | - | + | - |
| r-------- (040) | --------- (000) | - | - | - | - | - | + | - | - |
| r-------- (040) | --x------ (010) | - | - | - | - | - | + | - | - |
| r-------- (040) | -w------- (020) | - | - | - | - | - | + | - | - |
| r-------- (040) | -wx------ (030) | - | - | - | - | - | + | - | - |
| r-------- (040) | r-------- (040) | - | - | - | - | - | + | - | - |
| r-------- (040) | r-x------ (050) | - | - | - | - | - | + | - | - |
| r-------- (040) | rw------- (060) | - | - | - | - | - | + | - | - |
| r-------- (040) | rwx------ (070) | - | - | - | - | - | + | - | - |
| r-x------ (050) | --------- (000) | - | - | - | - | + | + | - | - |
| r-x------ (050) | --x------ (010) | - | - | - | - | + | + | - | - |
| r-x------ (050) | -w------- (020) | - | - | + | - | + | + | - | - |
| r-x------ (050) | -wx------ (030) | - | - | + | - | + | + | - | - |
| r-x------ (050) | r-------- (040) | - | - | - | + | + | + | - | - |
| r-x------ (050) | r-x------ (050) | - | - | - | + | + | + | - | - |
| r-x------ (050) | rw------- (060) | - | - | + | + | + | + | - | - |
| r-x------ (050) | rwx------ (070) | - | - | + | + | + | + | - | - |
| rw------- (060) | --------- (000) | - | - | - | - | - | + | - | - |
| rw------- (060) | --x------ (010) | - | - | - | - | - | + | - | - |
| rw------- (060) | -w------- (020) | - | - | - | - | - | + | - | - |
| rw------- (060) | -wx------ (030) | - | - | - | - | - | + | - | - |
| rw------- (060) | r-------- (040) | - | - | - | - | - | + | - | - |
| rw------- (060) | r-x------ (050) | - | - | - | - | - | + | - | - |
| rw------- (060) | rw------- (060) | - | - | - | - | - | + | - | - |
| rw------- (060) | rwx------ (070) | - | - | - | - | - | + | - | - |
| rwx------ (070) | --------- (000) | + | + | - | - | + | + | + | - |
| rwx------ (070) | --x------ (010) | + | + | - | - | + | + | + | - |
| rwx------ (070) | -w------- (020) | + | + | + | - | + | + | + | - |
| rwx------ (070) | -wx------ (030) | + | + | + | - | + | + | + | - |
| rwx------ (070) | r-------- (040) | + | + | - | + | + | + | + | - |
| rwx------ (070) | r-x------ (050) | + | + | - | + | + | + | + | - |
| rwx------ (070) | rw------- (060) | + | + | + | + | + | + | + | - |
| rwx------ (070) | rwx------ (070) | + | + | + | + | + | + | + | - |

1. На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнил табл. 3.2.

Table 2: Минимальные права для совершения операций от имени пользователей входящих в группу

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | d-wx——(030) | ———-(000) |
| Удаление файла | d-wx——(030) | ———-(000) |
| Чтение файла | d–x——(010) | -r——–(040) |
| Запись в файл | d–x——(010) | –w——-(020) |
| Переименование файла | d-wx——(030) | ———-(000) |
| Создание поддиректории | d-wx——(030) | ———-(000) |
| Удаление поддиректории | d-wx——(030) | ———-(000) |

# 5 Выводы

В данной лабораторной работе мне успешно удалось получить практические навыки работы в консоли с атрибутами файлов для групп пользователей.

# Список литературы

1. Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask) [Электронный ресурс]. 2023. URL: <https://habr.com/ru/articles/469667/>.

2. Права доступа к файлам и каталогам [Электронный ресурс]. 2023. URL: <https://younglinux.info/bash/rwx>.

3. Права доступа к файлам в Linux [Электронный ресурс]. 2023. URL: <https://losst.pro/prava-dostupa-k-fajlam-v-linux>.

4. Права доступа к файлам [Электронный ресурс]. 2023. URL: <https://docs.altlinux.org/ru-RU/archive/2.3/html-single/junior/alt-docs-extras-linuxnovice/ch02s08.html>.

5. Группы пользователей Linux [Электронный ресурс]. 2023. URL: <https://losst.pro/gruppy-polzovatelej-linux>.